

WEST Search History

[Hide Items](#)[Restore](#)[Clear](#)[Cancel](#)

DATE: Thursday, February 17, 2005

Hide?	<u>Set</u> <u>Name</u>	<u>Query</u>	<u>Hit</u> <u>Count</u>
		<i>DB=USPT; PLUR=YES; OP=OR</i>	
<input type="checkbox"/>	L5	L4 and (plaintext and ciphertext)	187
<input type="checkbox"/>	L4	L3 and (encrypt? and decrypt?)	1167
<input type="checkbox"/>	L3	L1 and L2	264514
<input type="checkbox"/>	L2	(non-associative adj operations or multiplication or division or subtraction or addition or inverse or exclusive)	2143806
<input type="checkbox"/>	L1	(stream adj cipher or block adj cipher or psuedo adj generator or random adj number or generator or keystream adj generator or combiner)	350991

END OF SEARCH HISTORY



US Patent & Trademark Office

[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)

 Search: ☒ The ACM Digital Library ☐ The Guide

stream ciphers

SEARCH

THE ACM DIGITAL LIBRARY


[Feedback](#) [Report a problem](#) [Satisfaction survey](#)
Terms used **stream ciphers**Found **10,584** of **150,138**Sort results
by

relevance

[Save results to a Binder](#)Try an [Advanced Search](#)Try this search in [The ACM Guide](#)Display
results

expanded form

[Search Tips](#)
☐ Open results in a new
window

Results 1 - 20 of 200

Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

Best 200 shown

Relevance scale ☐ ☐ ☐ ☐ ☐**1** [How to break Gifford's cipher \(extended abstract\)](#)

Thomas R. Cain, Alan T. Sherman

November 1994 **Proceedings of the 2nd ACM Conference on Computer and communications security**Full text available: [pdf\(1.14 MB\)](#)Additional Information: [full citation](#), [references](#), [index terms](#)

Keywords: Boston Community Information System, Gifford's cipher, algorithms over finite fields, correlation attack, cryptanalysis, cryptography, cryptology, filter generators, linear algebra over GF(2), linear feedback shift registers, matrix decompositions, primary rational canonical form, similar matrices, similarity transformations, stream ciphers

2 [Reception and posters: Securing media for adaptive streaming](#)

Chitra Venkatramani, Peter Westerink, Olivier Verscheure, Pascal Frossard

November 2003 **Proceedings of the eleventh ACM international conference on Multimedia**Full text available: [pdf\(233.56 KB\)](#)Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

This paper describes the ARMS system which enables secure and adaptive rich media streaming to a large-scale, heterogeneous client population. The secure streaming algorithms ensure end-to-end security while the content is adapted and streamed via intermediate, potentially untrusted servers. ARMS streaming is completely standards compliant and to our knowledge is the first such end-to-end MPEG-4-based system.

Keywords: MPEG-4, adaptive, encrypted, scalability, streaming, video server

3 [Security Mechanisms in High-Level Network Protocols](#)

Victor L. Voydock, Stephen T. Kent

June 1983 **ACM Computing Surveys (CSUR)**, Volume 15 Issue 2Full text available: [pdf\(3.23 MB\)](#)Additional Information: [full citation](#), [references](#), [citations](#)**4** [Low power scalable encryption for wireless systems](#)

James Goodman, Anantha P. Chandrakasan